IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI

UNITED STATES OF AMERICA

VS. NO.: 3:21-CR-107-NBB-RP

JAMARR SMITH, et al.

MEMORANDUM OF AUTHORITIES IN SUPPORT OF MOTION TO SUPPRESS

COMES NOW, the Defendant, Jamarr Smith, by and through the undersigned counsel, and files this memorandum of authorities in support of his Motion to Suppress, would state unto the Court as follows:

I. INTRODUCTION

This case arises out of the robbery of the United States Post Office in Lake Cormorant, Mississippi on February 5, 2018. For many months after the robbery, the government had no suspects; therefore, it used a newly-minted investigative technique involving a "geofence warrant" sent to Google, Inc. in the Fall of 2018. The geofence warrant required Google to search Location History data in approximately 592 million accounts of its users, and then produce data from those devices that were using Google services within a geographic area within a window of time. Unlike a typical warrant, this geofence warrant did not identify the defendants in this case in any way (i.e. it did not ask for Location History for Jamarr Smith) – and of course it did not identify the 592 million persons whose devices were searched. Instead, the warrant operated in reverse: it required Google to search the 592 million devices, and then allowed the government the discretion to obtain private information of interest.

Geofence warrants have been lately found to violate the Fourth Amendment on the basis that they are impermissible general warrants that unconstitutionally authorize a dragnet search of

Google users; thus making them, by definition, without probable cause, overbroad and lacking particularity as required by the Fourth Amendment. *See e.g. United States v. Chatrie*, 2022 WL 628905 (E.D. Va. March 3, 2022); *Matter of Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google*, 2020 WL 5491763 (N.D. Ill., July 8, 2020). This particular warrant was also defective due to misrepresentations in the probable cause statement, and the government's failure to use the "further legal process" that it said it would to obtain specific information about Google users made portions of the search warrantless and illegal.

Since the geofence warrant in this case was unconstitutional, it is void from its inception. The Court should suppress all evidence derived from that warrant as fruit of the poisonous tree.

II. FACTS

A. Underlying offense and application for warrant at issue

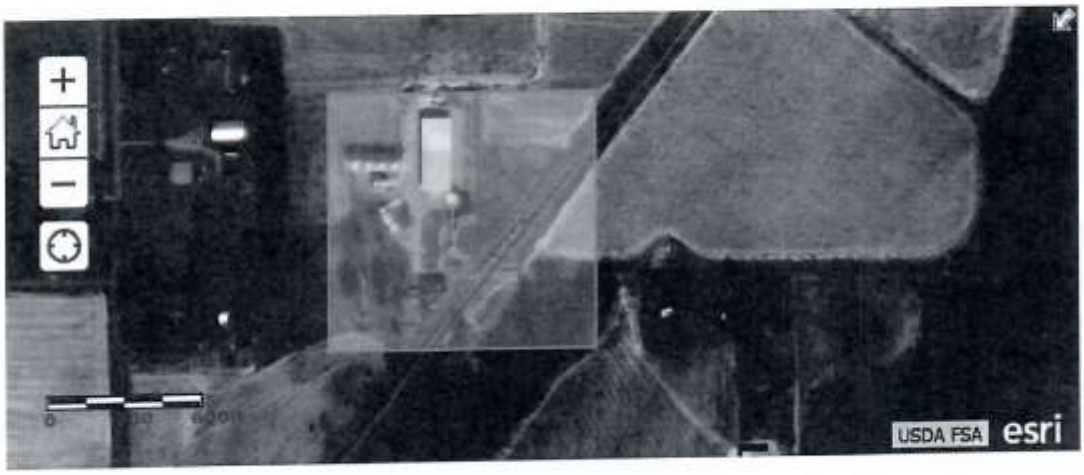
On February 5, 2018, the United States Post Office in Lake Cormorant, Mississippi was robbed. In the months following, it appears that the government was unable to develop any leads or suspects for the robbery.

Nine months after the robbery, on November 8, 2018, Inspector Todd Matney (hereinafter "Matney") of the United States Postal Inspection Service submitted an Application for a Search Warrant with attached affidavit to U.S. Magistrate Judge LeRoy Percy seeking information from Google. (Application, Exh. A; Affidavit, Exh. B).

The affidavit stated that "there is probable cause to believe that the Google accounts identified in Section I of Attachment A [to the affidavit], associated with a particular specified location at a particular specified time, contain evidence, fruits and instrumentalities of a violation of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee." (Exh. B, ¶ 2).

However the attachment identified no specific Google accounts of any particular individual; instead, attachment identified only a geographical box (i.e. geofence) of coordinates around the Lake Cormorant Post Office as follows:

The highlighted area in the below map is the area represented by the coordinates listed above and the location pinned in the middle of the highlighted area is the location of the Lake Cormorant Post Office.



(Exh. B, Attachment A). This square box covered approximately 98,192 square meters.[1]

The application explained that "Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location date from non-Android devices if the device is registered to a Google account and the user has location services enabled." (Exh. B, ¶ 8). The application went on to state that "[l]ocation data can assist investigators in understanding a fuller geographic picture and timeline, which may tend to identify potential witnesses, as well as possibly inculpating or exculpating account owners." (Exh. B, ¶ 9).

[1] For reference, a football field is slightly over 5,351 square meters. www.themeasureofthings.com

By way of background, "Location data" or "Location History" is maintained by Google through either its own Android operating system or through cell phones using a Google service or application such as Gmail, Search and Maps. *See Google Tracks Your Movements, Like it Or Not*, Associated Press (Aug. 13, 2018), https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb. Location History is a private journal of the device user's locations. (Report of Spencer McInvaille, Exh. D, p. 1). It is not a device-based setting; instead, it is an account-level setting where Google collects data across any device using the Google account. *Id.* One purpose of collecting Location History is to allow Google to better tailor searches and to enhance their user experience. *Id.* Perhaps Google's primary purpose for collecting this data is for advertising revenue:

> Location History data serves Google's advertising business by providing "store visit conversions" or "ads measurement" to businesses based on user location. . . . . Without identifying any individual user, this "store conversion" data can follow a particular ad campaign and identify "how many users who saw a particular ad campaign actually went to one of those stores." . . . . Google's "radius targeting" also allows—again without identifying any user—"a business to target ads to users that are within a certain distance of that business." . . . .
>
> * * *
>
> Indeed, Location History even allows Google to "estimat[e] ... where a device is in terms of elevation." . . . . [T]his capability helps locate someone in an emergency, or try to "determine if you are on the second [or first] floor of the mall" if the Google Maps directory has launched to help a user navigate indoors.

Chatrie, 2022 WL 628905 T *3. Google collects this information associated with each account in a "Sensorvault" to be used in advertisement marketing and many other purposes, including depicting on Google Maps whether a certain location is busy during particular hours. *Id.* at *4.

The affidavit contained a Probable Cause Statement which generally described the crime and that a couple of vehicles appeared to be involved with it. (Exh. B, ¶¶ 10-15). None of those

statements provided any specific probable cause to search a cell phone. The affidavit then contained this critical statement:

> 16. Postal Inspectors conducted a detailed review of video surveillance and it appears the robbery suspect is possibly using a cellular device both before and after the robbery occurs.

(Exh. B, ¶ 16). The affidavit also stated that, in the opinion of Matney, cell phones are used to plan crimes. (Exh. B, ¶ 18). That is the entire probable cause statement related to cell devices.

As is demonstrated by a review of the video referenced by the government, no robbery suspect is shown using a cellular device at any time.

Finally, the affidavit stated that the warrant would "identify which cellular devices were near the location where the robbery took place and may assist law enforcement in determining which persons were present or involved with the robbery under investigation." (Exh. B, ¶ 21). The affidavit stated that in response to the warrant, location data will:

> be provided by Google [which] will be identified only by a numerical identifier, without further content or information identifying the user of a particular device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and *will seek any additional information regarding those devices through further legal process*.

(Exh. B, ¶ 21b. (emphasis added)). Thus, the government recognized that "further legal process" was necessary to identify the specific users of the particular devices, i.e. "de-anonymized" data. As will be shown below, the warrant did not comply with this averment in the affidavit, and the government did not undertake "further legal process" to obtain the data.

B. Google's response to the warrant

The warrant itself, which was granted on November 8, 2018, established a three-step process where Google and the government collaborated to decide what information to produce.

(Warrant, Exh. C, p. 2). Defense expert Spencer McInvaille describes the three steps to be taken pursuant to the warrant:

II. Information to Be Provided by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts, which will be reviewed by law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee.

1. *Location information.* All location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings, **between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018**; Step 1

2. Any user and each device corresponding to the location data to be provided by the "Provider" will be identified only by a numerical identifier, without any further content or information identifying the user of a particular device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and will seek any additional information regarding those devices through further legal process.

3. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide additional location history outside of the predefined area for those relevant accounts to determine path of travel. This additional location history shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset. (The purpose of path of travel/contextual location points is to eliminate outlier points where, from the surrounding data, it becomes clear the reported point(s) are not indicative of the device actually being within the scope of the warrant.) Step 2

4. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide the subscriber's information for those relevant accounts to include, subscriber's name, email addresses, services subscribed to, last 6 months of IP history, SMS account number, and registration IP. Step 3

(Exh. D, p. 3).

1. Step 1

In Step 1, the warrant sought "all location data" in Google's possession for devices inside the geofence at the times in question. Because Google does not know which users have Location History enabled on their phones, it is required to search all accounts with Location History enabled. (Exh. D, Attachment II, ¶ 7 (stating "Google must conduct the search across all LH data to identify users with LH data during the relevant timeframe, and run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant. Google does not know which users may have such saved LH data before conducting the search and running the computations.)). Further, Google believes that only about 1/3 of its account holders have Location History enabled. (Exh. D, Attachment I, ¶ 13). Thus, Google searches all accounts whether they have Location History enabled or not – but the warrant only asked for "location data," which was only obtainable from those accounts with Location History enabled.

In October, 2018 (the month before the warrant was applied for), "there were approximately 592 million daily active users of Location History worldwide." (Exh. D, p. 2 & Attachment III, ¶ 3). Therefore, Google searched approximately 592 million accounts to determine whether they contained responsive data to the warrant. (Exh. D, pp. 2, 8 & Attachment II, ¶ 7). In other words, Google conducted a search of breathtaking scope in response to Step 1 of the warrant.

Notably, Google's search was much broader than that specifically sought by the warrant. Google actually produced date from a circular area that was approximately 378,278 square meters in area, not a 98,192 square meter box requested by the warrant. (Exh. D, pp. 6-7, 8). This is an area almost four times larger than the area sought to be searched by the warrant. (Exh. D, p.

8 (stating "the effective range of the geofence was larger than directed in the warrant request due to the manner in which data was requested by the Government.")). Therefore some devices identified may not have been in the actual geofence box sought by the warrant.

It is also important to note that just because a device is shown in the area of the search, it did not mean with certainty that the device was in fact within the radius of the search:

> 24. The location data points reflected in LH are estimates based on multiple inputs, and therefore a user's actual location does not necessarily align perfectly with any one isolated LH data point. Each set of coordinates saved to a user's LH includes a value, measured in meters, that reflects Google's confidence in the saved coordinates. A value of 100 meters, for example, reflects Google's estimation that the user is likely located within a 100-meter radius of the saved coordinates based on a goal to generate a location radius that accurately captures roughly 68% of users. In other words, if a user opens Google Maps and looks at the blue dot indicating Google's estimate of his or her location, Google's goal is that there will be an estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot.
>
> 25. Notwithstanding the confidence interval described above, if a user's estimated location (i.e., the stored coordinates in LH) falls within the radius of the geofence request, then Google treats that user as falling within the scope of the request, even if the shaded circle defined by the 68% confidence interval falls partly outside the radius of the geofence request. As a result, it is possible that when Google is compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore included in a data production) were in fact located outside the radius. To provide information about that, Google includes in the production to the government a radius (expressed as a value in meters) around a user's estimated location that shows the range of location points around the stored LH coordinates that are believed to contain, with 68% probability, the user's actual location.

(Exh. D, Attachment I, ¶¶ 24-25).

So, Google provided data concerning at least one account with Location History enabled

anywhere in the following circle:

and found at least one device with Location History enabled within that circle, and possibly outside that circle. (Exh. D, p. 7). The search of 592 million devices identified three devices.

This information was provided in an "anonymized" format which just provided a numerical identifier for the account, the type of account, time stamped location coordinates and the data source:

Device ID	Date	Time	Latitude	Longitude	Source	Maps Display Radius (m)
1091690859	2/5/2018	17:22:45 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091690859	2/5/2018	17:24:45 (-06:00)	34.9044587	-90.2159436	WIFI	98
1091690859	2/5/2018	17:27:04 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091690859	2/5/2018	17:27:35 (-06:00)	34.9044587	-90.2159436	WIFI	104
1091690859	2/5/2018	17:28:06 (-06:00)	34.9044587	-90.2159436	WIFI	92
1091690859	2/5/2018	17:28:42 (-06:00)	34.9044587	-90.2159436	WIFI	146
1091690859	2/5/2018	17:30:56 (-06:00)	34.9044587	-90.2159436	WIFI	347
1353630479	2/5/2018	17:58:35 (-06:00)	34.9044587	-90.2159436	WIFI	110
1577088768	2/5/2018	17:22:27 (-06:00)	34.9040345	-90.2155529	GPS	11
1577088768	2/5/2018	17:24:04 (-06:00)	34.9042131	-90.2155945	GPS	18
1577088768	2/5/2018	17:25:08 (-06:00)	34.9045528	-90.2151712	GPS	37

(Exh. D, p. 5).

The warrant specifically stated that any additional information obtained from Google after Step 1 would be with "further judicial process." (Exh. C).

2. Step 2

Step 2 of the process required by the warrant was as follows:

> 10. Second, the government reviews the de-identified production version to determine the device numbers of interest. If additional de-identified location information for a device in the production is necessary to eliminate false positives or otherwise determine whether that device is relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request (if authorized in that request).
>
> * * *
>
> 12. Finally, based on the de-identified data produced, the government can compel Google (if authorized in the request) to provide account-identifying information for the device numbers in the production that the government determines are relevant to the investigation. In response, Google provides account subscriber information such as the email address associated with the account and the name entered by the user on the account.

(Exh. D, Attachment I, ¶ 10). In other words, the government analyzed the "provided records," and demanded that Google "provide additional location history outside of the predefined area for those relevant accounts to determine path of travel;" – all without any additional judicial scrutiny that was promised at the end of Step 1. (Exh. C).

The government has produced no information regarding its actions in this step, and the defendants cannot evaluate what was or was not done in response to this step. (April 26, 2022 discovery letter, Exh. E (stating "1. Produce all documents and records . . . provided by Google as a result of the geofence warrants.); May 6, 2022 response to discovery letter, Exh. F (stating "we have already provided you all of the information in or possess that you requested in items 1 . . . ."); Exh. D, p. 8 (stating "Step 2 data was not contained in the discovery. . . .")). The defense

expert Spencer McInvaille is of the opinion that "there are communications for these requests and these communications provide significant insight into the process by which data was requested and responded to," and the government has not provided those communications. (Exh. D, p. 8).

3. Step 3

In Step 3, "upon demand" by the government and not through issuance of an additional warrant, Google produced "de-anonymized" (i.e. specific user) subscriber information. Google produced the following account information: "2165781.Key.csv", "bleek2004.AccountInfo.txt", "jamarrsmith33.AccountInfo.txt" and "permanentwavesrecords.AccountInfo.txt". (Exh. D, p. 8). This was contrary to the averments in the Matney affidavit that the government would undertake "further legal process" to obtain this data. (Exh. B, ¶ 21b.).

C. The government's use of the information provided by Google

The government used the information to apply other investigative techniques to obtain other evidence to prosecute the defendants herein. In other words, all significant evidence in this case was derived from information obtained from Google pursuant to this warrant.

III. DISCUSSION

A. Warrant application defect number one: misrepresentation of fact in probable cause statement.

The initial problem with the Application is that it contains a misrepresentation as to the *one essential* fact on which it is based: "Postal Inspectors conducted a detailed review of the video surveillance and it appears the robbery suspect is possibly using a cellular device both before and after the robbery occurs." (Exh. B, ¶ 16).

As the Court is well aware, the Fourth Amendment states "that no warrants shall issue, but upon probable cause." U.S. Const. amend. IV. Law enforcement personnel seeking the

issuance of a search warrant must present an affidavit containing facts sufficient to "provide the magistrate with a substantial basis for determining the existence of probable cause." *Illinois v. Gates*, 462 U.S. 213, 239 (1983). This factual showing for probable cause necessarily requires a truthful showing. *Franks v. Delaware*, 438 U.S. 154, 164–65 (1978) ("when the Fourth Amendment demands a factual showing sufficient to comprise 'probable cause,' the obvious assumption is that there will be a truthful showing."). Therefore, it is well-established that a person's "Fourth Amendment rights are violated if (1) the affiant, in support of the warrant, includes a false statement knowingly and intentionally, or with reckless disregard for the truth, and (2) the allegedly false statement is necessary to the finding of probable cause." *Winfrey v. Rogers*, 901 F.3d 483, 494 (5th Cir. 2018).

1. The affidavit contains a knowing and intentional false statement, or a statement with reckless disregard for the truth.

Simply stated, the video used by the government unquestionably does not show the "robbery suspect . . . possibly using a cellular device both before and after the robbery occurs." (Exh. B, ¶16). An accurate (and indeed exculpatory)[2] statement in the affidavit would be: "Postal Inspectors conducted a detailed review of the video surveillance and it does not show the robbery suspect using a cellular device before or after the robbery occurs."[3]

[2] The intentional or reckless omission of exculpatory information from a warrant application may amount to a Fourth Amendment violation. *See Hale v. Fish*, 899 F.2d 390, 400 n. 3 (5th Cir. 1990).

[3] The Court should be aware that the affidavit more than likely contained the statement about possible cellular device use (and not the more accurate exculpatory statement) because it was, upon information and belief, the product of a form or "go by" that the Justice Department provided to law enforcement agencies for use in obtaining geofence warrants. *See Chatrie*, 2022 WL628905 at *9 (discussing collaboration between Google and the Justice Department concerning geofence warrants). In hopes to discover this information, the defendants requested that the government "provide the template or form used by Todd Matney . . . for the geofence search warrant application in this case." (May. 25, 2022 discovery request, Exh. G). The government declined to produce this highly relevant information on the basis that it was "work

Smith acknowledges that Matney cannot be merely negligent in making statements in his affidavit. *Brewer v. Haynie*, 860 F.3d 819, 825 (5th Cir. 2017). Though an intentional misrepresentation or omission of material facts will certainly suffice, statements and omissions made with a reckless disregard for the truth will invalidate an affidavit and warrant. The Court may infer reckless disregard from circumstances evincing "obvious reasons to doubt the veracity" of the allegations. *St. Amant v. Thompson*, 390 U.S. 727, 731 (1968); *see also United States v. Tomblin*, 46 F.3d 1369, 1377 (5th Cir. 1995) (stating "recklessness can in some circumstances be inferred directly from the omission itself."). As demonstrated above, the statement in the affidavit was reckless at best.

Finally, the government may argue that Matney's use of the word "possibly" creates enough indefiniteness in the assertion that the Court may overlook it. However, a "technically true" statement is still a misrepresentation when "it manipulates the facts subtly." *United States v. Namer*, 680 F.2d 1088, 1093 n.10 (5th Cir. 1982). "Possible" use of a cellular device is a long way away from "no evidence" or "no indication" of use of a cellular device.

2. The false statement was important.

The second prong of *Franks* requires the Court to examine the affidavit with the false material set to one side and determine "whether the reconstructed affidavit would still support a finding of probable cause." *Kohler v. Englade*, 470 F.3d 1104, 1113 (5th Cir. 2006). To be clear,

---

product and therefore privileged." (May 26, 2022 discovery response, Exh. H). This would appear to be the first time the government has taken the position that a form or "go by" for a warrant contains "interviews, statements, memoranda, correspondence, briefs, mental impressions, personal beliefs" that are defined as work product by *Hickman v. Taylor*, 329 U.S. 495, 511 (1947).

If indeed the Matney affidavit was a form and not the product of particularized information that would establish probable cause, this is a further basis to suppress the evidence pursuant to *Franks*, 438 U.S. at 164–65.

and as will be discussed in more detail below, it is the defendants' position that the affidavit as originally submitted was completely lacking in probable cause to search the Google 592 million Google accounts at issue. Jamarr Smith is presenting this issue without conceding that the application and affidavit established probable cause in the first place.

Here is what the essential part of the reconstructed affidavit would look like with the "possibly using a cellular device" information from paragraph 16 removed:

- Cellular telephones may be used to determine the location of a device. (Exh. B, ¶¶6, 9).
- Google, Inc. collects this data. (Exh. B, ¶¶7-8).
- A robbery occurred at the post office in Lake Cormorant on February 5, 2018 during which Sylvester Cobbs was injured, and where three registered mail sacks were taken. (Exh. B, ¶¶10-14, 17).
- A maroon Hyundai Elantra and a white GMC Yukon are believed to be involved in the robbery. (Exh. B, ¶15).
- Matney believes, based upon his experience and training, that cell phones may have been used to plan the crime.[4] (Exh. B, ¶18).

In fairness to the defendants, the Court should also add the following exculpatory fact:

- Postal Inspectors conducted a detailed review of the video surveillance and it does not show the robbery suspect using a cellular device before or after the robbery occurs.

The government may contend that the statement about cellular device usage before and after the crime in question was supportive of a finding of probable cause to search cellular phones. Indeed, the above information (without the assertion that Matney observed cell phone use during the crime) transforms the affidavit into a "bare-bones" affidavit that is insufficient to

[4] As discussed in footnote 3 above, if the affidavit was in fact a form and not actually based on Matney's "experience and training" that cell phones may be used to plan crimes, then this element of probable cause should be ignored as well, rendering the application even more devoid of probable cause.

support probable cause as a matter of law.[5]

In particular, the only assertion of a nexus between this crime and a cell phone is the single statement that Matney believes, based upon experience and training, that cell phones may be used to plan crimes. This is inadequate because the Supreme Court has held that probable cause must be based on individualized facts, not group probabilities. *Ybarra v.* Illinois, 444 U.S. 85, 91 (1979). The Fifth Circuit has specifically found that such an assertion, *without more*, is insufficient to establish probable cause. *United States v. Broussard*, 80 F.3d 1025, 1034-35 (5th Cir. 1996) (stating "The so-called 'boilerplate' assertions that [defendant] complains of, which are based on the affiant's extensive experience and training and involve generalizations about the types of evidence that may be found in drug dealers' residences, do not undermine the reasonableness of reliance on the warrant. We do not mean to suggest that these types of generalizations, without more, are sufficient to render the officers' reliance objectively reasonable.").

Other jurisdictions have held on very similar facts that assertions that, based upon training and experience, persons tend to use cell phone to plan crimes is totally insufficient to support probable cause. In *United States v. Ramirez*, the court required that the Government make more specific allegations connecting the defendant, the cell phone searched, and the crime charged, instead of relying on generalizations that cell phones tend to contain evidence of crimes. *United States v. Ramirez*, 180 F. Supp. 3d 491 (W.D. Ky., 2016). The court noted that "[p]ossessing a cell phone during one's arrest for a drug-related conspiracy is insufficient by itself to establish a nexus between the cell phone and any alleged drug activity." *Id.* at 495.

[5] "'Bare bones' affidavits contain wholly conclusory statements, which lack the facts and circumstances from which a magistrate can independently determine probable cause." *United States v. Satterwhite*, 980 F.2d 317, 321 (5th Cir. 1992).

Similar reasoning should apply to the case at bar because law enforcement obtained data on the defendants' Google accounts where there was a lack of evidentiary nexus in this case, prior to the search," between the cell phone and any criminal activity. *Id.*, citing *United States v. Schultz*, 14 F.3d 1093, 1097 (6th Cir.1994). In *Ramirez*, the court analyzed an affidavit very similar to the one currently before the Court.

> Detective Petter's statement regarding her training and experience lacks any specific reference to the crime of drug trafficking. It generalizes that 'an individual' may have information on his or her phone that connects him or her to a crime, co-defendants or victims, rather than specifically connecting Ramirez, the crime with which he was charged, or any known information about communications made using this particular phone.

Id.[6] The court proceeded to find that the generalizations in the affidavit were insufficient even to trigger the good-faith exception. *Id.* at 496; *see also Commonwealth v. Broom*, 474 Mass. 486, 52 N.E.3d 81 (2016) (search warrant affidavit assertion that the affiant knows from training and experience that "cellular telephones contain multiple modes used to store vast amounts of electronic data" and that, in his opinion, "there is probable cause to believe that the [defendant's] cell phone and its associated accounts … will likely contain information pertinent to this investigation" is a "general, conclusory statement" that "adds nothing to the probable cause calculus"). Here, Matney's affidavit omits an assertion or belief that a cell phone was used by a suspect as a tool in this robbery, as the Magistrate Judge typically sees when authorizing a wire tape or search warrant of a specific cell phone in a drug case.

Thus, the reconstructed warrant did not support a finding a probable cause, and was invalid.

[6] Of course, the Court will easily see the additional distinction between affidavits seeking access to a specific, identified person's cell phone and the affidavit at issue in this case: The government could not and did not identify a specific cell phone that it wanted to search – which only compounds the defectiveness of the application.

B. Warrant application defect number 2: the government did not undertake "further legal process" to obtain the de-anonymized user information that it said it would, making Steps 2 and 3 a warrantless search.

In both the affidavit supporting the warrant application and the warrant itself, the government stated following Step 1 of the warrant, it was going to request anonymous location data "identified only by a numerical identifier, without any further content or information identifying the user of a particular device," and recognized that it could not obtain the specific user information without "further legal process." (Exh. B, ¶ 21b., Exh. C.). The government undertook no further legal process to obtain the specific user information; thus the government's obtaining the de-anonymized information was a warrantless search by the very terms of the application.

As will be discussed further below, the discretion to the government as to what information it wanted to get fails the Fourth Amendment particularly requirement and is unconstitutional in its own right. But the fact that the government conducted a warrantless search also requires suppression of the information obtained.

The Supreme Court has held that a search must be confined to the terms and limitations of the warrant authorizing it. *Bivens v. Six Unknown Agents of the FBI*, 403 U.S. 388, 394 n. 7 (1971). Further, searches and seizures "'conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment-subject only to a few specifically established and well delineated exceptions.'" *Thompson v. Louisiana*, 469 U.S. 17, 19–20 (1984)(per curiam) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967) (footnotes omitted)).

The "terms and limitations" of the application for the warrant required the government to undertake "further legal process" to obtain the Step 3 information. The government's failure to

do this rendered the warrant *per se* unreasonable under the Fourth Amendment. It is unknown what specific exception the government might assert as an exception to the warrantless search exclusion, but the government could not seriously argue that it was "objectively reasonable"[7] for it to obtain this information without a warrant when the warrant application and accompanying affidavit specifically stated that it would obtain such a warrant.

C. The warrant violated the Fourth Amendment.

The crucial fact about this warrant was that it was not a search of people in the vicinity of the Lake Cormorant post office on the day and times in question; it was a search of all Google users with Location History enabled. Thus, the warrant required Google to conduct an epic dragnet of hundreds of millions of private accounts to determine if any one of them contained data of interest. This is prohibited by the Fourth Amendment.

1. Cell phones and the data contained in them are granted heightened protection by the Fourth Amendment.

The Supreme Court has stated: the "Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' ... [that] allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014). Further, when discussing cell phones, the Court stated that "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives." *Id.* at

[7] The Supreme Court has recognized an exception to the warrantless search prohibition where "'the exigencies of the situation' make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." *Carpenter v. United States*, ___ U.S. ___, 138 S. Ct. 2206, 2222 (2018). "Such exigencies include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence." *Id.* (citing *Kentucky v. King*, 563 U.S. 452, 460 (2011)). Courts "have approved warrantless searches related to bomb threats, active shootings, and child abductions." *Id.* Obviously, those conditions did not exist here.

395. Indeed, the "term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Id.* at 393. In addition to the numerous types of information available on cellphones, "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity," enabling phones to hold "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* at 393–94. As such, a "cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." *Id.* at 396–97 (emphasis in original); *see also United States v. Oglesby*, 2019 WL 1877228, at *5 (S.D. Tex. Apr. 26, 2019) (finding that "the protections given to a cell phone must be at least equal to, if not greater than, the protections set out for houses").

There can be no serious contention that a person does not have an expectation of privacy as to their Location History contained in their cell phones, and the fact that this information may be held by a third-party like Google has no effect on that principle. *See Carpenter,* 138 S.Ct at 2219, 2223 (holding that the government's access of GPS location information from cell phone providers invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements" and noting that there could soon be more sophisticated systems similarly protected.). *Carpenter* specifically rejected application of the third-party doctrine because cell phone users did not truly voluntarily share their cell phone data with their service provider because "carrying [a cell phone] is indispensable to participation in modern society." *Id.* at 1220 (citing *Riley*, 573 U.S. at 384-85).

Accordingly, the information contained in and through cell phones can only be searched pursuant to a lawful search warrant, and probable cause receives a heightened level of scrutiny.

Riley, 573 U.S. at 403.

2. The warrant lacked probable cause and was overbroad.

The Supreme Court defines "probable cause" as "a fair probability that contraband or evidence of a crime will be found in a particular place. *Gates*, 462 U.S. at 238. A warrant is overbroad if the government lacks probable cause to search. *United States v. Sanjar*, 876 F.3d 725, 735 (5th Cir. 2017). Thus, the two aspects of the Fourth Amendment require that (1) a warrant provide sufficient notice of what the agents may seize and (2) probable cause exist to justify listing those items as potential evidence subject to seizure. *Williams v. Kunze*, 806 F.2d 594, 598-99 (5th Cir. 1986).

Here, the warrant did not identify any person about whom it sought information from Google, nor did it only search devices around the Lake Cormorant post office on the date and time in question. It required Google to search all accounts (whether the accounts had Location History enabled or not - approximately 592 million – an epic dragnet),[8] and then the government decided what to seize.[9] There can be no doubt that, the government did not have probable cause

[8] This is truly a record-setting search, involving a number of persons that dwarfs the number of persons searched in any other reported criminal opinion. Even "tower dumps," which are the subject of controversy in their own right, impact no more than thousands of persons, and usually only hundreds. *See e.g. United States v. James*, 2019 WL 325231 at * 3 (D. Minn., Jan. 25, 2019) ("hundreds if not thousands" of cell phone users).

[9] This particular defect with the warrant is best described by the court in *Chatre*:

> This warrant, for instance, contains no language objectively identifying which accounts for which officers would obtain further identifying information. Nor does the warrant provide objective guardrails by which officers could determine which accounts would be subject to further scrutiny. Nor does the warrant even simply limit the number of devices for which agents could obtain identifying information. Instead, the warrant provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—without ever needing to return to a neutral and detached magistrate for approval.

to search hundreds of millions of Google users' accounts. In fact, the government did not have probable cause to search one Google user's account because the government had no identifiable suspects, much less a suspect that it believed was using Location History on his or her phone. *Ybarra* requires that there be some evidence of a person's involvement in the suspected crime in order for the Fourth Amendment to allow the seizure of that person – or, by analogy the seizure of that person's things, such as Location History, in which the person has a constitutionally protected expectation of privacy. *Ybarra*, 444 U.S. at 91. So the government cannot rely on the generalized statement that "persons who commit crimes use cell phones" to establish probable cause. Probable cause must be based on individualized facts, not group probabilities. *Id.*

Ybarra, as demonstrated by the court in *Chatrie*, is particularly apposite here. In *Ybarra*, the government obtained a search warrant for any and all persons located in The Aurora Tap Tavern at the time of execution of the warrant because of the belief that somebody therein, plus the bartender "Greg," had narcotics on their person. *Ybarra*, 444 U.S. at 88. The Court found that "[t]here is no reason to suppose that, when the search warrant was issued on March 1, 1976, the authorities had probable cause to believe that any person found on the premises of the Aurora Tap Tavern, aside from 'Greg,' would be violating the law." *Id.* at 90. Nonetheless, Ybarra, a patron in the tavern, was found to have heroin on his person. The Court found that the police might have had probable cause to search the tavern itself, but certainly not Ybarra's person, stating "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Id.* at 91 (citing *Sibron v. New York*, 392 U.S. 40, 62–63 (1968). Further,

> [w]here the standard is probable cause, a search or seizure of a

---

Chatrie, 2022 WL 628905 at *25.

> person must be supported by probable cause particularized with respect to that person. This requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be.

Id.

The court in *Chatrie* relied on *Ybarra* in finding that the warrant was based on "inverted probable cause:"

> that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby. In essence, the Government's argument rests on precisely the same "mere propinquity to others" rationale the Supreme Court has already rejected as an appropriate basis for a warrant. [*Ybarra*, 444 U.S. at 91.] This warrant therefore cannot stand.

Chatrie, 2022 WL 628905 at *24; *see also In re Search of Information Stored at Premises Controlled by Google,* 481 F. Supp. 3d at 753 (invalidating the geofence warrant because it provided the government "unlimited discretion to obtain from Google the device IDs . . . of anyone whose Google-connected devices traversed the geofences (including their vaguely defined margins of error), based on nothing more than the 'propinquity' of these persons to the Unknown Subject at or near the time" of the criminal activity) (citing *Ybarra,* 444 U.S. at 91). Thus, the importance of *Chatrie* is that the court ruled that the government must establish probable cause to search each of the 592 million accounts – which the government could never do.

Indeed, it is difficult to imagine what probable cause could justify searching 592 million devices, but here there was no probable cause at all. The complete absence of probable cause makes the warrant fatally overbroad from the beginning. In other words, the government's effort to search all accounts with Location History enabled rendered the warrant an improper modern-

day general warrant. *See Warden v. Hayden*, 387 U.S. 294, 313 (1967) (Douglas, J., dissenting).

3. The warrant lacked particularity.

The Fourth Amendment requires that warrants "particularly describe[e]" the place to be searched and the things to be seized. The Supreme Court has interpreted this to require that the warrant particularly describe the place to be searched and the items to be seized so that nothing is left to the discretion of the officer in executing the warrant. *Marron v. United States,* 275 U.S. 192, 196 (1927); *Coolidge v. New Hampshire,* 403 U.S. 443, 467 (1971).

Here, the geofence warrant left it up to Google and the government to negotiate which users would have their account information searched – the hallmark of an unparticularized warrant. The warrant provided for a three-step process which permitted the government to use its discretion as to what it wanted to have.

Step One of the warrant did not provide clear information on what could be seized and ensnared people outside the geofence box in the warrant. Google did not search only the square geofence in the warrant – instead it searched a much larger area that was almost four times the size of the box and in which it had only a 68% probability that a given device was in that area – meaning that there was a 32% chance that some data provided was not in the geofence at all. Therefore, Google (in its own discretion) provided much more information than the actual warrant sought. In other words, Google and the government impermissibly used their discretion to decide what to search and which devices to identify as within the search area – all of which was well beyond what a particular warrant permits. No judge signed off on seizure of data for devices outside the square geofence. The Court should also consider that Google states that only 1/3 of its account holders have Location History enabled in the first place. (Exh. D, Attachment I, ¶ 13). Nonetheless, Google searched all accounts whether they had location history enabled or

not.

Step Two and **Step Three** gave the government discretion as to which Google users would be the subject of further scrutiny – all without "further legal process as required by the application and the warrant itself. First, the government required that Google provide additional information outside the scope of Step 1 of the warrant "location history outside of the predefined area . . . . [that] shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account" identified in Step 1. (Exh. C). When Google produced the anonymous information regarding devices, the government decided what was "relevant" and then obtained de-anonymized information without returning to the court for an additional authorization. Other courts have denied geofence warrant applications on exactly this basis. *In Matter of Search of Info. Stored at Premises Controlled by Google*, the Court stated:

> This Court cannot agree that the particularity requirement is met here by virtue of the proposed geofences being narrowly tailored in a manner justified by the investigation. Attachment B to the proposed warrant, listing the items to be seized, does not identify any of the persons whose location information the government will obtain from Google. As such, the warrant puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that traversed the geofences. A warrant that meets the particularity requirement leaves the executing officer with no discretion as to what to seize, *Stanford*, 379 U.S. at 485, 85 S.Ct. 506, but the warrant here gives the executing officer unbridled discretion as to what device IDs would be used as the basis for the mere formality of a subpoena to yield the identifying subscriber information, and thus, those persons' location histories.

Matter of Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d at 754.

Therefore, the warrant fails the particularity requirement because the government and Google decided what to seize, and no objective observer could look at the warrant and ascertain which specific accounts the government had authority to search and seize. This violates the

Fourth Amendment.

D. The good faith exception does not apply.

The government may argue that the good faith exception to the exclusionary rule created by *United States v. Leon*, 468 U.S. 897 (1984) should excuse the clear defectiveness of this warrant and prevent application of the exclusionary rule. However, in *Leon*, the Court outlined four circumstances where the good faith exception does not apply, two of which are clearly applicable here:

1) the warrant is based on recklessly false statements;

2) the affidavit lacks substantial basis to determine probable cause; and

3) the warrant was facially deficient.

Leon, 468 U.S. at 914-915.

The first factor is discussed above. The warrant application clearly contains a recklessly false statement concerning cell phone usage by one of the participants in the robbery.

As to the second factor and as discussed extensively above, the warrant not only lacked a "substantial" basis to determine probable cause, it lacked any probable cause at all. Certainly, any judge would have denied the warrant application had he or she known that the warrant authorized Google to search 592 million user accounts.

Finally, the third factor is clearly met as discussed above because the warrant was totally lacking in probable cause.

Therefore, the good faith exception does not apply, and the Court should exclude any evidence obtained by this warrant, and also any evidence derived from this warrant as fruit of the poisonous tree.

IV. CONCLUSION

Based upon the forgoing, the Court should suppress the evidence that the government obtained pursuant to the warrant to Google at issue, as well as any other evidence derived from that information as fruit of the poisonous tree. Jamarr Smith requests any further relief the Court may find warranted in the premises.

RESPECTFULLY SUBMITTED,

JAMARR SMITH

HICKMAN, GOZA & SPRAGINS, PLLC
Attorneys at Law
Post Office Drawer 668
Oxford, MS 38655-0668
(662) 234-4000 telephone
(662) 234-2000 facsimile
glewis@hickmanlaw.com

BY: */s/ Goodloe T. Lewis*
GOODLOE T. LEWIS, MSB # 9889

CERTIFICATE OF SERVICE

I, GOODLOE T. LEWIS, attorney for JAMARR SMITH, do hereby certify that I have on this date electronically filed the foregoing document with the Clerk of Court using the ECF system which sent notification of such filing to all counsel of record, including:

Robert Mims
Office of the US Attorney
900 Jefferson Avenue
Oxford, MS 38655
rmims@usadoj.gov

DATED: November 4, 2022.

/s/ Goodloe T. Lewis
GOODLOE T. LEWIS

GOODLOE T. LEWIS, MSB # 9889
HICKMAN, GOZA & SPRAGINS, PLLC
Attorneys at Law
Post Office Drawer 668
Oxford, MS 38655-0668